International Journal of Research and Development in Applied Science and Engineering (IJRDASE)
ISSN: 2454-6844

Review on the Application of Blockchain Technology in Indian Context

Ajay Kumar Bharti[1],Sumaiya[2],Mr. Hannan Ansari[1]
[1]Computer Science and Engineering Department
Bansal Institute of Engineering and Technology, Lucknow, India
[2]Computer Science and Engineering Department
Maharishi University of Information Technology, Lucknow, India

Abstract-Blockchain technology is a decentralized distributed system meant for secure computation and information sharing platform free from any central authority that enables multiple authoritative domain which do not trust each other, to cooperate, coordinate and collaborate in rational decision making process. Bitcoin is pioneer crypto currency platform that uses blockchain technology but over the time it has moved beyond Bitcoin and has successfully bypassed to other application domain. Beside Bitcoin, Ethereum, Hyperledger and Corda have emerged as a successful distributive computing platform. Today we have different blockchain application in public sector, finance, supply-chain, IoT. Major consortium like Enterprise EthereumAlliance, Hyperledger and R3 are formed with aim to come up with business solution. In many industries people think blockchain will be transformative. Financial sector is most enthusiastic in adopting blockchain followed by supply chain management. Blockchain is closely looked at in India too. In 2018 Reserve Bank of India (RBI) has issued a white paper in order to identify the potential application areas of blockchain in Indian banking. NITI Aayog is working on national strategy for blockchain which will identify the area where country can implement blockchain. However,blockchain is still new and facing various challenges like scalability, security and network size issue, limited transaction loads, and high (computational) costs and privacy leakage.

Keyword: - Public blockchain, Private Blockchain, Bitcoin

1. INTRODUCTION

With traditional methods for recording transactions and tracking assets, participants on a network keep their own ledgers and other records. This traditional method can be expensive, partially because it involves intermediaries that charge fees for their services. It's clearly inefficient due to delays in executing agreements and the duplication of effort required maintaining numerous ledgers. It is also vulnerable because if a central system (for example, a bank) is compromised, due to fraud, cyber attack, or a simple mistake, the entire business network is affected.

Blockchain is peer-to-peer network where multiple nodes are interconnected and each node maintains local copy of blockchain (ledger), system task is to ensure that every copy is consistent with global copy of blockchain. The blockchain architect gives participants the ability to share a ledger that is updated, through peer-to-peer replication every time a transaction occurs. Peer-to-Peer replication means each participant (node) in the network acts as both a publisher and a subscriber. Each node can receive or send transactions to other nodes, and the data is synchronized across the network as it is transferred. The blockchain network is economical and efficient, because it eliminates duplication of effort and reduces the need for intermediaries.

Blockchain also provides immutability through cryptographic hash function. Each block contains hash of previous block which ultimately create a chain of blocks. Each block contain encrypted digitally signed append only logs of transaction verified by peer nodes .A block may have multiple transactions invoked by users. Blockchain are broadly categorized under public (permissionless) or private (permissioned) blockchain. Public blockchain works in open environment over a large network of participant where users have anonymous identity e.g. Bitcoin and Ethereum. Private Blockchain involves only few ten to a few hundred known participant and users with permissions can join the network, write or send transactions to the blockchain like Hyperledger. Possibility for inclusion of Blockchain technology is huge hence it is closely looked by increasing number of organizations and companies. Blockchain is envisioned to have wide range of application such as trade finance, supply chain and logistic, medical data exchange or IoT asset tracking.

In India also blockchain has garnered positive response both from public and private sector. Though crytocurrency and Bitcoin is snubbed by Indian government but blockchain technology is endorsed, Indian finance minister Arun Jaitley in his budget speech 2018[1] mentions that India foresee blockchain as potential cutting-edge technology. In domestic market blockchain could be use for various services like land registry, farm insurance, digital certificate and e-governance.

2. BLOCKCHAIN TECHNOLOGY

Blockchain is a sequence of blocks, which holds a complete list of transaction records like conventional public ledger [2].Blockchain design makes this technology immutable and secure. Once the transaction is committed after the consensus of all peer nodes the transaction will not altered. Each block is identifiable by a hash, generated using the SHA256 cryptographic hash algorithm on the header of the block[3]. Each block references a previous block, also known as the parent block, in the “previous block hash” field, in the block header. A hash, also known in long form as cryptographic hash function, is a mathematical algorithm that maps data of arbitrary size to a bit string of a fixed size. In the case of SHA 256, the result is a string of 32 bytes. The resultant 32 bytes makes it effectively impossible to reverse the output, since the function was designed to be a one-way function (Schneier, 2004) [4]. Hash functions are collision-free too. That means it’s impossible to find two messages that hash to the same hash value [5]. Therefore, when given a compact hash, one can confirm that it matches a particular input data. Blocks can be identified from their hash, serving two purposes; identification and integrity verification. Santoshi Nakamto has proposed transaction be hashed in a Merkle Tree with only the root included in the block hash[6]. .It is tree structure where the leaf node contain the hash of the document and its intermediate node contain the hash combination of its left and right child, which makes a change in anyone hash value reflected in all subsequent hash value. Merkle tree in peer-peer network ensures that data block received is unaltered and no peer node can lie about a transaction.Transaction in blockchain is same as any transaction in distributed system, it follow ACID property. Few blockchain uses scripting languages for transaction likes Bitcoin while Ethereum uses smart contract for various application. Blockchain is said to be pioneering technology to realize smart contracts. Blockchain works in distributed and decentralized environment where each node works independently, thus transactions are verified and committed to the ledger by means of *consensus* (agreement).The role of the consensus algorithm is to gets all nodes in the system to agree upon the decision. If a node commits a block, all other nodes also append same copy of the block. Consensus protocol like PoW[7], PoS[8], Raft[9], PBFT[10] are employed in blockchain.

Table 1: Blockchain Platforms

Platform	Type	Salient Features
Ethereum[11]	Public	Its blockchain with a built-in Turing-complete programming language, allowing clients to write smart contracts and decentralized applications and executed in Ethereum Virtual Machine (EVM). Ethereum currently is the most common platform for developing smart contracts.
Hyperledger[12]	Private	Developed under Linux Foundation is first open source blockchain platform that run distributed applications written in standard, general-purpose programming languages like Node.js, Go, Java, Python.
Quorum[14]	Private	Quorum is private platform of Ethereum to support enterprise requirement. Quorum uses a voting based consensus algorithm Quorum Chain, the critical addition to Quorum are security and data privacy but it retain EVM.
Ziliqa[15]	Public	Zilliqa is sharding based blockchain that achieved network sharding and could successfully scale up to 3,600 nodes.
Corda[13]	Private	Developed by R3 , it’s a distributed ledger platform for permissioned network designed specifically considering requirement of financial institutions.

3. CURRENT BLOCKCHAIN APPLICATIONS WORKING IN DIFFERENT INDUSTRIES

A) Supply Chain

Blockchain provide food traceability and security by tracking food from source to retailer store providing certified end-to end chain of custody. Several companies like Skuchain, Provenance, Walmart, and Everledger provide blockchain based solutions to supply chain management.

B) Trade Finance

Global trade relies heavily on trade finance. Any trading involves lending, issuing letters of credit, factoring, export credit and insurance, bill of exchange. Traditional trade finance challenge are tons of documents needed between importer, exporter, shipper, banks, etc, each entities stores copies of the same document of information which requires constant reconcile against each other database. Blockchain in trade finance promises real time visibility, automate business processes that are transcending organizational boundaries, enhance trust through Smart Contract, speeding up of transaction settlement time (which currently takes days) and reduced transaction fees.

C) Health Care Services

Blockchain is promising in healthcare industry; it could contribute in varying sectors like health data exchange, new medical claim process, pharmacy supply chain provenance and traceability or clinical trial management.

D) Trade Logistics

Trade logistic challenges include error-prone information, border-delays, manual data collection, excess inventory, and lack of shipment visibility etc.IBM and Maersk led TradeLens blockchain solution that provide shipping solution that bring various parties together to share trades processing document.

E) Digital Identity

Every business and social interaction is driven by person's identity. Identity compromise of several attributes like name, age, work history, financial history, address history etc. Digital Identity system already exists in our system it reduces paper documentation but vulnerable to data breaches. The digital identity need to ensure self-sovereign principle i.e. individual should have full control and ownership of his/her identity and develop distributed trust model among multiple different vendors who are using individual identities. Blockchain solution Hyperledger Indy provides distributed ledger for creating and using independent digital identity.

Table 2: Blockchain Project taken up in India

Year	Blockchain Project/Consortium/Enterprises
2017	SBI along with other leading Indian bank has launch consortium BankChain with tech companies IBM ,Intel among others to developed financial enterprise solution for services like KYC etc.
2018	Yes Bank with Hyperledger Distributed Ledger Technology(DLT) developed blockchain solution to provide digitize automated vendor financing system for Bajaj Electricals
2018	TechMahindra partnered with Microsoft to create Distributed Ledger based solution to build a blockchain technology aimed at managing spam calls
2018	Kerala government K-DISC (Kerala Development and Innovation Strategic Council) has decided to use blockchain in supply chain management of milk, vegetables and fish with the states.
2018	Telangana Government partnered with TechMahindra to launch India's first Blockchain District that facilitates and promote blockchain startup and companies
2017	NITI Aayog has announced blockchain project IndiaChain for the country for various purposes like land records keeping and public goods disbursement.
2018	NITI Aayog partnered with Oracle India announces pilot project on blockchain based platform for India's domestic pharmaceutical supply chain services to combat fake drug distribution

4. RECENT START-OFF BLOCKCHAIN PROJECTS IN INDIA

Blockchain is received positively in India (Table 2), both government and industry is taking keen interest in its adoption opportunities. NITI Aayog in 2018 started working on national strategy for blockchain to identify the area where India can implement the technology. RBI issued white paper (2018)[16] on implementation of Blockchain technology in the areas of banking and finance in India with suggested roadmap for the adoption of technology to Indian banking system in area of trade finance, KYC, supply chain finance, bill discounting, monitoring of consortium accounts, servicing of securities and mandate management system. NASSCOM and Avasant jointly published India Blockchain Report 2019[17] found out that banking; insurance sector, financial sector and public sector are key player who plunges into blockchain projects and use cases. Report also states that nearly half of states in India have initiated blockchain projects.

5. KEY CHALLENGES

Blockchain is a nascent technology and concern is raised by industry in adopting blockchain to mainstream. From technical perspective scalability of blockchain is still not up to a mark with market demands. Blockchain platform services like Ethereum process 7-10 transaction per seconds which is far less to available VISA or MasterCard that process nearly 4,500 transaction per second. Blockchain also faces interoperability issue because there are varied blockchain systems each with distinct and complex architect which makes it unable to interoperate. Integration of blockchain with other system like IoT or AI is also not developed yet. Blockchain maintain user's pseudonymous identity however it cannot guarantee transaction privacy and it's been subjected to several attacks and security breaches[18].Skepticism of regulatory bodies to regulate blockchain is another major hurdle for industries like financial services and banks[19].

6. CONCLUSION

Blockchain has shown its potential for transforming traditional systems and leveraging many industries with its key characteristics: decentralization, audibility, anonymity and immutability. In this paper, we presented comprehensive overview of blockchain, its architecture, application areas where blockchain and emerging opportunities for blockchain in India.

REFERENCES

[1] Union Budget 2018: 5G, AI, Blockchain gets special mention in Arun Jaitley’s speech. (n.d.). Retrieved May 2019, 4 , from Financial Express: www.financialexpress.com

[2] Lee KuoChuen, David, (2015), Handbook of Digital Currency,ed., Elsevier, https:// EconPapers.repec.org/ RePEc: eee:monogr: 9780128021170.

[3] Naik, R. P. (September 2013). Optimising the SHA256 Hashing Algorithm for Faster and More Efficient Bitcoin Mining. London: UCL

[4] Gipp,B.,Meuschke,N.,andGernandt,A.(2015)."Decentralized trusted time stamping using the crypto currency bitcoin". arXiv preprint arXiv:1502.04015.

[5]FIPS PUB 180-2. “SHA256 Standard.” (2002). National Institute of Standard Technology , 86-92.

[6] Merkle, R. C. (1998). A Digital Signature Based on a Conventional Encryption Function .Springer, (pp. 370-378). Verlag.

[7] Dwork,Cynthia;Naor, Moni (1993). "Pricing via Processing, Or, Combatting Junk Mail, Advances in Cryptology". CRYPTO’92: Lecture Notes in Computer Science No. 740. Springer: 139–147.

[8] Diego Ongaro, J. O. (June 2014). In search of an understandable consensus algorithm. USENIX Annual Technical Conference (pp. 305-320). Philadelphia: ACM

[9] P. Vasin, “Blackcoins proof-of-stake protocol v2,” 2014. [Online]. Available:https://blackcoin.co/blackcoin-pos-protocol-v2-whitepaper.pdf

[10] Miguel Castro and Barbara Liskov. Practical Byzantine fault tolerance and proactive recovery. ACM Trans. Comput. Syst., 20(4):398–461, November 2002.

[11] Buterin, V. (2004). A Next-Generation Smart Contract and Decentralized Application Platform. Ethereum White Paper.

[12] Hyperledger. (n.d.). Retrieved May 3, 2019, from www.hyperledger.org

[13] Richard Gendal Brown, James Carlyle, Ian Grigg, Mike Hearn,” Corda: An Introduction” August, 2016

[14]Quorum Whitepaper. (n.d.). Retrieved from github: https://github.com/ethereum/wiki/wiki/White-PaperUSA, 2016, pp. 839–858.

[15] Zilliqa. (n.d.). Retrieved May 3, 2019, from www.zilliqa.com

[16]Institute for Development and Research in Banking Technology. (2018). Application of Blockchain Technology to Banking and Financial Sector in India. RBI.

[17] NASSCOM Avasant India Blockchain Report . India (2019).

[18] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, “Hawk:The blockchain model of cryptography and privacy-preserving smart contracts,” in Proceedings of IEEE Symposium on Security and Privacy(SP), San Jose, CA,

[19] PwC's Global Blockchain Survey 2018. (n.d.). Retrieved May 3, 2019, from www.pwc.com